Bundesstrafgericht
Tribunal pénal fédéral
Tribunale penale federale
Tribunal penal federal

Numéro de dossier: BB.2019.245

Décision du 26 janvier 2021
Cour des plaintes

Composition	Les juges pénaux fédéraux Roy Garré, président, Cornelia Cova et Patrick Robert-Nicoud, la greffière Daphné Roulin
Parties	**A.,** représenté par Me Maurice Harari et Me Laurent Baeriswyl, recourant **contre** **MINISTÈRE PUBLIC DE LA CONFÉDÉRATION,** intimé
Objet	Extension de l'instruction (art. 311 al. 2 CPP); admission de la partie plaignante (art. 118 ss en lien avec l'art. 104 al. 1 let. b CPP)

Faits:

A. Le 11 décembre 2017, le « groupe Bb. » et C., administrateur président avec signature individuelle de B. SA, ont déposé, par l'entremise de Me E., une « dénonciation formelle (art. 301 al. 1 CPP) » auprès du Ministère public de la Confédération (ci-après: MPC) à l'encontre de F. pour les infractions, à tout le moins, de soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143bis CP), services de renseignements économiques (art. 273 CP) et violation du secret de fabrication ou de secret commercial (art. 162 CP; act. 1.16).

B. Le 1er mai 2018, A., représenté par Me Harari, a appuyé les conclusions contenues dans la lettre susmentionnée du 11 décembre 2017 de C. et du « groupe Bb. » (act. 1.17).

C. Le 19 novembre 2018, le MPC a ouvert une instruction pénale contre F. pour service de renseignements économiques au sens de l'art. 273 CP, procédure référencée sous n. SV.18.0492 (cf. act. 1.22).

D. Par lettre du 4 février 2019 adressée au MPC, A. par l'entremise de Me Harari et Me Baeriswyl s'est constitué partie plaignante, tant au pénal qu'au civil, dans le cadre de cette procédure (act. 1.24).

Le 5 février 2019, le MPC a refusé ladite constitution (lettre du 5 février 2019, act. 1.25).

Les 18 février, 20 mars et 27 mai 2019, A. a requis l'extension de l'instruction à l'infraction de soustraction de données au sens de l'art. 143 CP et a réitéré sa constitution en tant que partie plaignante (act. 1.27, 1.29 et 1.31).

Le 12 juin 2019, le MPC a refusé d'étendre la procédure à l'infraction de soustraction de données (art. 143 CP) et a indiqué que A. ne pouvait pas revêtir la qualité de partie plaignante dans le cadre de la procédure ouverte (act. 1.32).

A. a demandé au MPC de revoir sa position (lettre du 24 juillet 2019, act. 1.35).

Par acte du 11 octobre 2019, avec indication de la voie de recours, le MPC a maintenu sa position (act. 1.1).

E. Le 24 octobre 2019, A. – représenté par Me Harari et Me Baeriswyl –

interjette recours contre la décision précitée auprès de la Cour des plaintes du Tribunal pénal fédéral (act. 1). Il conclut en substance, sous suite de frais et dépens, principalement, à l'annulation de la décision du 11 octobre 2019 du MPC, à ce que l'instruction pénale contre F. du chef de soustraction de données (art. 143 CP) soit ouverte, respectivement étendue, au renvoi de la cause au MPC pour instruction en ce sens, à son admission en qualité de partie plaignante dans la procédure ouverte, respectivement étendue, et de réserver son droit de solliciter la répétition des actes d'instruction accomplis en son absence. À titre subsidiaire, il prend les mêmes conclusions à la différence que, à la place que l'instruction soit ouverte, il conclut à ce que la cause soit renvoyée au MPC pour qu'il ouvre, respectivement étende, l'instruction pénale contre F. du chef de soustraction de données (art. 143 CP).

F. Dans le cadre de l'échange d'écritures, le MPC conclut au rejet du recours (act. 4 et 16). Par réplique du 16 décembre 2019, A. persiste dans les termes de son recours (act. 14).

G. Par lettre spontanée du 8 mai 2020 (act. 18), le recourant transmet à la Cour un document du 30 avril 2020 rendu par le MPC dans le cadre d'une autre procédure pénale référencée sous le n. SV.17.1802 (instruction pénale ouverte le 8 décembre 2017 contre A. et C.). En substance, il ressort de cet acte que la Procureure fédérale en charge de la cause l'informait de sa décision d'exploiter les données extraites du serveur de B. SA ainsi que toutes les preuves dérivées de celles-ci (act. 18.1).

Invité à se déterminer, le MPC indique que ce document n'influence pas le sort du recours et maintient que celui-ci doit être rejeté (act. 20).

Le recourant a ensuite fait part de ses déterminations spontanées (act. 23 et 25).

Les arguments et moyens de preuve invoqués par les parties seront repris, si nécessaire, dans les considérants en droit.

La Cour considère en droit:

1.

1.1 La Cour des plaintes du Tribunal pénal fédéral examine d'office la recevabilité des recours qui lui sont adressés (v. GUIDON, Die Beschwerde gemäss Schweizerischer Strafprozessordnung, 2011, n. 546 et les références citées).

1.2 Les décisions du MPC peuvent en principe faire l'objet d'un recours devant la Cour des plaintes du Tribunal pénal fédéral (art. 393 al. 1 let. a CPP et art. 37 al. 1 de la loi fédérale du 19 mars 2010 sur l'organisation des autorités pénales de la Confédération [LOAP; RS 173.71]). Le refus du MPC d'étendre l'instruction de la procédure à une autre infraction s'apparente à une décision de non-entrée en matière (arrêt du Tribunal fédéral 6B_1276/2019 du 27 février 2020 consid. 3.1 et la référence citée; v. décision du Tribunal pénal fédéral BB.2016.376-384 du 2 février 2018 consid. 2.4.5 et la référence citée: dans ces cas, il s'agit d'un refus du ministère public d'étendre l'instruction à d'autres prévenus), laquelle peut faire l'objet d'un recours devant la Cour de céans (art. 322 al. 2 CPP par renvoi de l'art. 310 al. 2 CPP, cf. art. 309 al. 1 CPP). Conformément à l'art. 393 al. 2 CPP, le recours peut être formé pour violation du droit, y compris l'excès et l'abus du pouvoir d'appréciation, le déni de justice et le retard injustifié (let. a), la constatation incomplète ou erronée des faits (let. b) ou l'inopportunité (let. c).

1.3 Interjeté le 24 octobre 2019, le recours a été déposé dans le délai de dix jours dès la notification de la décision attaquée (cf. art. 384 et 396 al. 1 CPP), soit le 14 octobre 2019, et a été ainsi formé en temps utile.

2. Le recours formé par A. contient deux volets, à savoir, d'une part, l'extension de l'instruction de la procédure ouverte par le MPC à l'infraction de soustraction de données (art. 143 CP) et, d'autre part, son admission en qualité de partie plaignante dans le cadre de la procédure pénale ouverte contre F. Il y a lieu de traiter ces deux aspects distinctement et d'examiner à chaque fois leur recevabilité, en particulier en ce qu'il concerne la qualité pour recourir.

Extension de l'instruction

3. Il convient d'examiner la qualité pour recourir de A. relative à sa requête d'extension de l'instruction à l'infraction de soustraction de données (art. 143 CP).

3.1 La qualité pour recourir de la partie plaignante (art. 118 al. 1 CPP; *partie* à la

procédure au sens de l'art. 104 al. 1 let. b CPP) contre une ordonnance de classement, de non-entrée en matière ou de refus d'étendre l'instruction – est subordonnée à deux conditions cumulatives: ses droits doivent être directement touchés par l'infraction (cf. art. 115 al. 1 CPP) et elle doit faire valoir un intérêt juridiquement protégé à l'annulation de la décision (cf. art. 382 al. 1 CPP). En règle générale, seul peut se prévaloir d'une atteinte directe le titulaire du bien juridique protégé par la disposition pénale qui a été enfreinte (ATF 141 IV 1 consid. 3.1 p.5; 129 IV 95 consid. 3.1 et les arrêts cités). Par ailleurs, l'intérêt doit être actuel et pratique (arrêt du Tribunal fédéral 1B_157/2019 du 9 juillet 2019 consid. 2).

3.2 En l'espèce, le recourant conclut à une extension de l'instruction à l'infraction de soustraction de données au sens de l'art. 143 CP. Cette disposition vise la protection du droit du bénéficiaire légitime de disposer de ses données et de ses logiciels (TPF 2016 28 consid. 2.1). Cette infraction a ainsi pour but de protéger les intérêts privés. A. allègue en particulier que F. a soustrait illégalement l'intégralité du serveur du groupe Bb., lequel contenait de nombreuses données relatives au groupe mais également le concernant (act. 1 n. 72 p. 19). Il ressort du dossier qu'est également litigieux la soustraction des boîtes e-mails de A. et C. La question pourra souffrir de demeurer ouverte de savoir si le recourant est le bénéficiaire légitime de disposer de ces données, respectivement s'il est directement touché et donc lésé. En effet, il n'y pas lieu d'approfondir la question de la qualité pour recourir de A. dans la mesure où, au vu des motifs développés ci-après, le recours doit de toute manière être rejeté.

4. Le recourant fait valoir que la décision querellée contient une non-entrée en matière implicite en violation de l'art. 310 CPP.

4.1

4.1.1 Conformément à l'art. 311 al. 2, 1ère phrase, CPP, le ministère public peut étendre l'instruction à d'autres prévenus et à d'autres infractions, l'art. 309 al. 3 CPP étant alors applicable. L'extension de l'instruction suppose que les conditions pour l'ouverture d'une instruction (art. 309 al. 1 CPP) soient réalisées en ce qui concerne les autres faits, respectivement les autres personnes, visés (GRODECKI/CORNU, Commentaire romand, 2ème éd. 2019, n. 15 ad art. 311 CPP).

4.1.2 Si le ministère public refuse la requête d'extension, sa décision s'apparente à une non-entrée en matière au sens de l'art. 310 CPP (arrêt du Tribunal fédéral 6B_1276/2019 du 27 février 2020 consid. 3.1 et la référence citée). Conformément à l'art. 310 al. 1 let. a CPP, le ministère public rend immédiatement une ordonnance de non-entrée en matière s'il ressort de la

dénonciation ou du rapport de police que les éléments constitutifs de l'infraction ou les conditions à l'ouverture de l'action pénale ne sont manifestement pas réunis. Selon la jurisprudence, cette disposition doit être appliquée conformément à l'adage « *in dubio pro duriore* ». Celui-ci découle du principe de la légalité (art. 5 al. 1 Cst. et 2 al. 1 CPP en relation avec les art. 309 al. 1, 319 al. 1 et 324 CPP; ATF 138 IV 86 consid. 4.2 p. 91) et signifie qu'en principe, un classement ou une non-entrée en matière ne peuvent être prononcés par le ministère public que lorsqu'il apparaît clairement que les faits ne sont pas punissables ou que les conditions à la poursuite pénale ne sont pas remplies. La procédure doit se poursuivre lorsqu'une condamnation apparaît plus vraisemblable qu'un acquittement ou lorsque les probabilités d'acquittement et de condamnation apparaissent équivalentes, en particulier en présence d'une infraction grave. En effet, en cas de doute s'agissant de la situation factuelle ou juridique, ce n'est pas à l'autorité d'instruction ou d'accusation mais au juge matériellement compétent qu'il appartient de se prononcer (ATF 143 IV 241 consid. 2.2.1 p. 243; 138 IV 86 consid. 4.1.2 p. 91 et les références citées; cf. récemment arrêt du Tribunal fédéral 6B_641/2020 du 8 septembre 2020 consid. 4.1).

L'établissement de l'état de fait incombe principalement au juge matériellement compétent pour se prononcer sur la culpabilité du prévenu. Le ministère public et l'autorité de recours n'ont dès lors pas, dans le cadre d'une décision de classement d'une procédure pénale, respectivement à l'encontre d'un recours contre une telle décision, à établir l'état de fait comme le ferait le juge du fond. Des constatations de fait sont admises au stade du classement, dans le respect du principe « *in dubio pro duriore* », soit dans la mesure où les faits sont clairs, respectivement indubitables, de sorte qu'en cas de mise en accusation ceux-ci soient très probablement constatés de la même manière par le juge du fond. Tel n'est pas le cas lorsqu'une appréciation différente par le juge du fond apparaît tout aussi vraisemblable. Le principe « *in dubio pro duriore* » interdit ainsi au ministère public, confronté à des preuves non claires, d'anticiper sur l'appréciation des preuves par le juge du fond. L'appréciation juridique des faits doit en effet être effectuée sur la base d'un état de fait établi en vertu du principe « *in dubio pro duriore* », soit sur la base de faits clairs (ATF 143 IV 241 consid. 2.3.2 p. 244 et les références citées; cf. arrêt du Tribunal fédéral 6B_1276/2019 du 27 février 2020 consid. 3.1 et la référence citée).

4.1.3 En vertu de l'art. 6 al. 1 CPP, les autorités pénales recherchent d'office tous les faits pertinents pour la qualification de l'acte et le jugement du prévenu (maxime de l'instruction). Par ailleurs, selon l'art. 7 al. 1 CPP, elles sont tenues, dans les limites de leurs compétences, d'ouvrir et de conduire une procédure lorsqu'elles ont connaissance d'infractions ou d'indices permettant de présumer l'existence d'infractions (principe du caractère impératif de la

poursuite).

4.2 A teneur de l’art. 143 al. 1 CP, se rend coupable de soustraction de données celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part.

Les données informatiques doivent avoir une protection spéciale – au moyen de mesures techniques, et non seulement en raison d’obstacles légaux, moraux ou contractuels – démontrant la volonté de la personne ayant légalement accès aux données d'empêcher que des tiers n'accèdent à ses données ou de restreindre cet accès. La personne non autorisée doit pouvoir reconnaître que les données sont protégées. Mis à part le verrouillage de locaux et d'armoires, par exemple, l'utilisation d'un chiffrement, de codes d'accès, de clefs biométriques ou de mots de passe est également une manifestation de cette intention. La norme pénale ne s'applique donc pas à une attaque contre des données non protégées ou à leur utilisation illicite. Enfin, il n'est pas exigé que le propriétaire possède de meilleures compétences informatiques que l'auteur, ni que la protection ait une efficacité particulière (TPF 2016 28 consid. 2.1 et les références citées).

Il n'y a pas de mesures suffisantes dans le cas d'un employé qui ne rencontre aucune mesure de sécurité spécifique lui entravant l'accès aux données détenues par son employeur, si ce n'est une barrière morale. Les instructions, les interdictions orales ou écrites, ou encore les mesures d'organisation visant à séparer les fonctions au sein du personnel ne constituent pas des mesures de sécurité suffisantes au sens de l'art. 143 CP (TPF 2016 28 consid. 2.1 et les références citées).

4.3 Les griefs des parties sont les suivants:

4.3.1 D’après le recourant, non seulement les faits relatifs à la soustraction de données (art. 143 CP) ne sont pas clairs, mais de plus il existe un doute quant à la qualification de soustraction de données des faits reprochés à F. Le MPC reconnaitrait lui-même que certains documents étaient protégés par mots de passe, de sorte qu’il convient de déterminer si ces documents étaient librement accessibles par F. ou si, à défaut de code d’accès confié à F., celui-ci ne pouvait pas y accéder. En sus, le recourant explique que le MPC a lui-même admis que les informations divulguées par F. ne provenaient pas exclusivement des boîtes e-mails de A. et C. En effet, F. a lui-même indiqué être en possession de tout le serveur du groupe Bb., par l’entremise de l’informaticien G. qui lui aurait remis une copie. Au vu des

allégations contradictoires de G., il appartient au MPC de déterminer de quelle manière F. s'est approprié les données informatiques confidentielles contenues sur le *serveur* du groupe Bb. Le recourant soutient que ces éléments ne peuvent être occultés par le MPC. Au surplus, d'après le recourant, il n'a notamment jamais été déterminé, si F. possédait les mots de passe des boîtes e-mails de A. et C., ni dans quelles circonstances ces mots de passe lui auraient été donnés, ni à quel contenu ils permettaient d'avoir accès. En conséquence, en l'absence de vision claire des faits, le MPC est empêché de rendre à ce stade une ordonnance de non-entrée en matière, doit ouvrir une instruction pénale et investiguer la source des données soustraites par F. et le mode d'accès utilisé par celui-ci, avant de se prononcer sur la réalisation de l'élément constitutif objectif des données spécialement protégées (act. 1 n. 41 à 65 p. 16 à 18; act. 14).

4.3.2 Le MPC soutient que l'élément constitutif objectif des *données spécialement protégées* fait défaut, puisque « F. était précisément en possession des mots de passe des ordinateurs de C. et A. » (act. 1.1). Selon le MPC, les deux rapports, soit celui du 19 juin 2015 préparé par la société H. et celui du 24 mars 2015 préparé par la société I., démontrent que F. a bien transféré un grand nombre d'informations provenant de la société B. SA, notamment en ayant eu accès à la boîte mail de A. et C., dont il avait les mots de passe. Le MPC se réfère au « *written statement* » de A. devant la police thaïlandaise qui a fait mention d'un courriel reçu de F. dans lequel ce dernier indiquait être principalement en possession des courriels de A. et C. De plus, les faits parus dans le « *J.* » se basent principalement sur le contenu des courriers auxquels F. avait accès. Enfin, le MPC souligne qu'il n'apparaît nulle part que le reste des données volées provenant du serveur de B. SA était protégé par des mots de passe (act. 1.1, 4 et 16).

4.4 A titre liminaire, il sied de rappeler les relations entre les différents protagonistes. F. a été engagé auprès de la société B. SA aux alentours des années 2007 et 2009, de sorte qu'il était employé de cette société. C. est l'administrateur président de la société B. SA avec signature individuelle (cf. registre du commerce). Au moment des faits, soit lors de la potentielle soustraction de données au printemps 2011, A. travaillait également au sein de B. SA; par ailleurs, selon le registre du commerce, il a été un administrateur de B. SA avec signature collective à deux de juin 2011 à mai 2018. B. SA et F. ont résilié avec effet immédiat leur relation contractuelle au 15 avril 2011 (« *employment agreement* » act. 1.4 [le document n'est pas signé par les parties, mais selon le recourant il reflète leur accord, dès lors qu'ils s'étaient intégralement entendus sur les termes]; « *termination agreement* » act. 1.2; audition de F. du 23 février 2017 en qualité de personne à donner des renseignements dans la procédure pénale n. SV.15.0969: act. 1.18).

En outre, afin d'avoir une conception claire du contexte dans lequel intervient le présent recours, il sied d'énumérer les différentes procédures pénales topiques ouvertes devant le MPC. En 2015, le MPC a, suite aux dénonciations MROS, ouvert une procédure pénale contre deux anciens agents publics malaisiens, sous le numéro de procédure le n. SV.15.0969. L'ouverture de cette instruction pénale serait une conséquence de la révélation dans la presse des données de B. SA dont F. était en possession (recours act. 1 n. 13 à 15, 17 et 18). En outre, le MPC a ouvert le 8 décembre 2017 une nouvelle instruction pénale (n. SV.17.1802) contre A. et C. pour, notamment, soupçons de gestion déloyale (art. 158 CP), escroquerie par métier (art. 146 al. 1 et 2 CP), corruption active d'agents publics étrangers (art. 322^{septies} al. 1 CP), faux dans les titres (art. 251 CP) et blanchiment d'argent aggravé (art. 305bis ch. 1 et 2 CP) (cf. act. 25.1 p. 2). Enfin, le présent recours est interjeté dans le cadre de la procédure pénale n. SV.18.0492 ouverte contre F. pour service de renseignements économiques au sens de l'art. 273 CP (cf. let. C).

4.5

4.5.1 En l'espèce, les écritures du recourant documentent peu sur la gestion réelle du parc informatique de B. SA, de la configuration des appareils ou encore des procédés techniques (physique ou électronique). La gestion des données en lien avec les employés de la société n'est également pas abordée. Ainsi, non seulement, l'argumentation développée par le recourant se limite à des généralités en se contentant d'affirmer que les données étaient protégées au moyen de mots de passe, mais de plus relève des contradictions. D'une part, le recourant argumente qu'une protection avait été effectivement mise en place interdisant l'accès des données à F., mais d'autre part il soutient que la procédure pénale devrait encore être instruite sur la manière dont F. a eu accès à ces données. Dans la mesure où il allègue que ses propres données auraient été « volées », il appartiendrait à A. lui-même de répondre à ces questions, ou du moins avec l'aide de la société B. SA qui est titulaire du serveur. En outre, on peine à discerner quel acte concret d'instruction permettrait de fournir de plus amples informations, autres que le concerné et la société B. SA, étant rappelé que cette dernière gère son parc informatique, dont A. revendique désormais le « hackage ». Le recourant ne suggère d'ailleurs pas sur quel complément d'instruction devrait procéder le MPC. Il n'apparaît donc pas qu'il existerait des éléments matériels permettant de retenir que les données obtenues par F. étaient spécialement protégées contre un accès indu, étant rappelé que F. était employé de B. SA et non un quelconque tiers.

Il ressort encore du dossier plusieurs éléments relatifs à l'éventuelle soustraction des données opérée par F., notamment en rapport avec la question de savoir si les données étaient spécialement protégées. Il convient

donc de les examiner.

4.5.2 A l'appui de sa thèse, le recourant a produit deux rapports, l'un de la société H. du 19 juin 2015 (act. 1.7) et le second de I. du 24 mars 2015 (act. 1.8). Ces rapports portent sur la boîte e-mail et l'ordinateur professionnels de F. Ces rapports attestent notamment que F. aurait enregistré des données sensibles de B. SA sur Dropbox (act. 1.8 p. 2 et 14), qu'il aurait transféré des données de sa boîte e-mail professionnelle à celle privée (act. 1.7 n. 4 et 23), que les documents envoyés par F. lors des faits de chantage n'apparaitraient pas sur les documents qu'il s'est auto-envoyé (act. 1.7 n. 4 et 25), que dans les vingt-quatre heures précédant son départ, F. aurait connecté des clés USB et un Blackberry à son ordinateur de la société (act. 1.7 n. 4, 16, 19 et 20) ou encore que les dossiers de B. SA auraient pu être copiées subrepticement en utilisant la « D. SA LAN » via l'ordinateur de A. (act 1.8 p. 2 et 5).

Comme l'a soulevé à juste titre le MPC, ces rapports diligentés par le recourant, respectivement C. ou B. SA, n'apportent pas plus d'éclaircissements sur les mesures de sécurité mises en place au sein de ladite société B. SA ni la protection que F. a dû surmonter pour avoir accès aux données. Ces rapports ne constituent donc pas des éléments matériels démontrant que les données étaient spécialement protégées.

4.5.3 En 2015, F. a été condamné par la justice thaïlandaise à une peine privative de trois ans pour des faits de chantage (act. 1.3). Il ressort du jugement thaïlandais que, entre le 22 juillet 2013 et le 17 octobre 2013, soit après la fin des rapports de travail, F. a menacé A. de révéler les informations confidentielles de la société B. SA, s'il ne lui versait pas une certaine somme. Cette condamnation s'est fondée notamment sur des échanges d'e-mails intervenus en 2013 entre F. et ses ex-employeurs (A. et C.). Aux termes de l'un de ces e-mails, F. a indiqué: « j'ai en ma possession tous les détails, même les plus importants, des débuts de B. SA jusqu'à mon départ. Ce sont plusieurs milliers de documents, principalement des e-mails. […] Les dernières semaines avant mon départ de Londres, j'ai été tellement mal traité et même plus que cela que j'ai dû me protéger en prenant ce que j'appellerais une assurance-vie », BB.2020.248-249 act. 1.4 annexe 6). Par ailleurs, dans le cadre de cette procédure pénale thaïlandaise, A. a indiqué à la police thaïlandaise comment F. avait eu accès aux informations de la société (« *written statement of the Petitioner, Complainant or Witness* » du 8 mai 2015, p. 8): « *In addition to his responsibility for information technology management in the Company, Mr. F. specifically assisted Mr. C. and me. For example, if we traveled abroad for business purposes and wanted to have some documents to be sent to our computers. This was normally in accordance with the principle of a specific action for each time under the*

express understanding that Mr. F. would be able to access our computers when he was assigned to do so for the specific purposes only. In order for Mr. F. to perform his duties, it was necessary for him to access Mr. C.'s and my computer (in accordance with the specific purpose for each time and under the express understanding only). Therefore, we gave him our password » (BB.2019.248-249 act. 1.4 annexe 3).

Au vu de ces éléments, F. aurait eu le mot de passe de A. et C. pour accéder à leur ordinateur (« *computer* »). Certes, une protection spéciale (mot de passe) avait été mise en place, néanmoins elle ne s'appliquait pas à F. La seule barrière pour F. était d'être limité aux seules instructions données par A. et C., ce qui ne constitue pas des mesures de sécurité suffisantes au sens de l'art. 143 CP. Dans cette constellation, la condition objective de protection spéciale des données contre un accès indu de F. ne serait pas réalisée. Les déclarations de A. se contredisent: il a d'abord prétendu dans la procédure thaïlandaise que F. avait accès à son ordinateur et à celui de C. avant de se raviser dans la présente procédure suisse et de préciser qu'il ne savait pas à quoi F. avait accès grâce aux mots de passe donnés. De tels atermoiements enlèvent toute crédibilité à A. Le recourant n'apporte d'ailleurs guère d'explications sur l'existence de ces deux versions. Il se borne à défendre qu'il appartient au MPC d'instruire notamment les circonstances dans lesquelles ces mots de passe auraient été remis à F. et le contenu auquel ils auraient prétendument permis d'avoir accès. Enfin, les deux récits de A. s'opposent diamétralement aux déclarations de F. ou de G. (v. ci-dessus consid. 4.5.4).

4.5.4 Il sied encore d'examiner les déclarations de F. en 2017 selon lesquelles le serveur du groupe Bb. lui aurait été remis par l'informaticien de cette société par amitié (audition de F. du 23 février 2017 en qualité de personne à donner des renseignements dans la procédure pénale n. SV.15.0969 [act. 1.18]). F. a expliqué: « Je me suis également occupé de la supervision de l'installation de tout le parc informatique de B. SA, étant précisé que les serveurs se trouvaient à Genève (p. 3). […] Pour ce faire j'ai travaillé avec G. qui exploitait une société informatique basée en Valais (p. 4) […] sauf erreur en mai ou en juin 2011, j'ai voulu avoir une assurance au cas où, raison pour laquelle j'ai contacté l'informaticien G., avec qui j'avais travaillé pour la mise en place du parc informatique de B. SA et je lui ai demandé si par amitié me mettre à disposition une copie du serveur de B. SA. G. a accepté de me rendre ce service et il m'a donc remis une copie du serveur de B. SA en me précisant que le serveur avait été détruit ou les données effacées sur ordre de C. Je pense que G. avait dû garder une copie du serveur car sans cela il n'aurait pas pu m'en remettre un exemplaire vu cette destruction ou cet effacement de données » (p. 6 à 7). L'informaticien G. a quant à lui réfuté les déclarations de F. et de lui avoir remis « quoique ce soit » (act. 1.19 p. 5

audition de G. en qualité de personne appelée à donner des renseignements du 31 mars 2017 dans le cadre de la procédure pénale n. SV.15.0969). En audition de confrontation du 5 juillet 2017, les deux intéressés ont confirmé leurs déclarations respectives sans permettre de clarifier les faits (act. 1.20).

Certes, comme soulevé par le recourant, le MPC n'a pas mentionné les auditions précitées dans la décision entreprise, toutefois, on comprend que le MPC a retenu que celles-ci n'influençaient pas son appréciation. Les deux intéressés, F. et G., ayant été confrontés sans résultat, l'on ne discerne pas au vu du dossier ce qui permettrait de retenir l'une de ces déclarations plus qu'une autre, ou quelle mesure d'instruction permettrait de le faire. De surcroît, il s'agit de versions qui s'opposent à celles présentées par A. dans son recours (v. consid. 4.3.1) ou lors de ses déclarations devant les autorités thaïlandaises (v. consid. 4.5.3). La Cour constate que le dossier comprend autant de versions que de personnes impliquées. En l'absence d'éléments matériels suffisants fournis par B. SA, titulaire des données sur la sécurité de son parc informatique, ou par A. sur la gestion sécuritaire du parc informatique, force est de constater que des déclarations contradictoires s'opposent sans permettre de retenir une version plutôt qu'une autre.

4.5.5 Le recourant produit encore un article de presse paru le 19 novembre 2019 dans un média suisse, lequel présente une interview récente de K. Il explique qu'elle a rédigé en tant qu'intervenante principale des articles sur « J. » en lien avec les faits de la cause et peut être considérée comme l'interlocutrice privilégiée de F. Le recourant fait ainsi référence au passage suivant de son interview: *« 2014 kam ein Whistleblower, ein Ex-Manager des Ölkonzerns B. SA, der schon 2009 mit 1MDB ein Joint Venture gegründet hatte. Der Mann hatte reichlich Material, unter anderem Hunderttausende E-mails, von den Servern kopiert* » (act. 14.1 p. 3). D'après le recourant, cela constitue un élément supplémentaire démontrant à tout le moins qu'une partie des données litigieuses ont été soustraites du serveur de B. SA, de sorte qu'il appartient au MPC d'instruire cet aspect (réplique act. 14 p. 3). La Cour de céans ne voit pas les éléments qu'une journaliste en tant que témoin indirect pourrait apporter qui ne figureraient pas déjà au dossier. Un tel grief doit être écarté.

4.5.6 Il ressort encore du recours que F. se serait engagé contractuellement à une utilisation diligente et précautionneuse des moyens de communication et appareils électroniques et à garder confidentielle toute information en lien avec le groupe Bb. (act. 1 n. 2 et les annexes citées). Il aurait garanti n'avoir gardé aucun document, support ou copies contenant des données confidentielles (cf. act. 1 n. 7 et l'annexe citée). Il sied de souligner que de telles clauses contractuelles ne permettent pas de protéger des données contre un accès indu au sens de l'art. 143 al. 1 CP (v. consid. 4.2). L'accès

doit être interdit au moyen de mesures techniques, ce qu'une interdiction contractuelle n'est pas. Ce grief doit également être écarté.

4.5.7 A titre superfétatoire, il sied de relever que le vocabulaire utilisé par le MPC pour définir les données, dont F. a été en possession, ne constitue pas un élément permettant de démontrer que l'infraction de soustraction de données (art. 143 CP) est réalisée. En d'autres termes, il n'est pas pertinent pour l'examen de l'énoncé de fait légal que le MPC fasse état dans une demande de ressource à la Police judiciaire fédérale du 13 août 2015 que des données informatiques ont été « volées » par F. (cf. act. 1 n. 19 en lien avec l'act. 1.12) ou que dans un document la Procureure fédérale en charge de la procédure n. SV.17.1802 fasse référence à la jurisprudence relative à des « données obtenues illicitement par des particuliers » (act. 18 en lien avec l'act. 18.1).

4.5.8 Vu l'objet du présent recours, il n'y a pas lieu d'entrer en matière sur la lettre du MPC du 30 avril 2020 faisant part – dans la procédure pénale ouverte contre A. et C. référencée sous le n. SV.17.1802 – de la volonté de procéder à l'exploitation des données litigieuses *in casu* (v. let. G). Cette lettre a d'ailleurs donné lieu à un recours auprès de la Cour de céans. Dans la mesure où les griefs du recourant auraient eu trait au présent recours, ceux-ci ont été développés ci-dessus.

4.5.9 En résumé, le MPC a déterminé que les données dont F. avait eu accès étaient principalement issues des boîtes e-mails de A. et C., dont F. avait les mots de passe. Le MPC a apprécié les éléments au dossier et les déclarations des parties pour établir les faits, bien qu'aucune instruction n'ait encore été ouverte. Il a fait une fausse application du principe « *in dubio pro duriore* » en procédant en réalité à une appréciation des preuves qui relève de la compétence du juge du fond. Toutefois, la décision du MPC de refus d'étendre l'instruction doit être confirmée au motif que les déclarations contradictoires s'opposent sans éléments matériels permettant de retenir une version plutôt qu'une autre. Ainsi, au vu des éléments du dossier, le recourant ne rend pas l'existence de faits pénalement répréhensibles au regard de l'art. 143 CP (notamment l'existence d'une protection spéciale) plus vraisemblable ou tout au moins aussi vraisemblable qu'un acquittement.

4.6 Il s'ensuit que le recours portant sur l'extension de l'instruction doit être rejeté dans la mesure de sa recevabilité.

Refus d'admission de partie plaignante

5. Le recourant dispose de la qualité pour recourir contre la décision du MPC de lui refuser l'admission de la qualité de partie plaignante dans le cadre de

la procédure menée par le MPC. En effet, la décision entreprise lèse le recourant dans son intérêt juridiquement protégé, en tant qu'il est exclu de la procédure (arrêt du Tribunal pénal fédéral BB.2012.18-23 du 22 novembre 2012 consid. 2.1).

6. Sur le fond, il sied de distinguer l'admission de la partie plaignante dans le cadre de l'art. 143 ou de l'art. 273 CP.

6.1 Concernant l'art. 143 CP, il sied de relever que le MPC a refusé à juste titre d'étendre l'instruction à cette infraction et à ce sujet le recourant a eu la possibilité d'être entendu dans le cadre de cette procédure devant une autorité avec plein pouvoir d'examen (v. *supra* consid. 1.2). Par conséquent, la question ne mérite pas d'être approfondie (v. *supra* consid. 4).

6.2 Dans le cadre de la procédure instruite pour soupçons de service de renseignements économiques (art. 273 CP), le recourant ne conclut pas à être admis en qualité de partie plaignante. A titre superfétatoire, il sied de préciser qu'il ne revêt également pas la qualité de partie plaignante au regard de l'art. 273 CP (cf. décision du Tribunal pénal fédéral BB.2019.248 consid. 6.2).

6.3 Concernant le refus d'admission de partie plaignante, le recours est également mal fondé et par conséquent rejeté.

7. En tant que partie qui succombe, le recourant supporte, en application de l'art. 428 al. 1 CPP, les frais de la présente procédure. Ceux-ci prendront en l'espèce la forme d'un émolument fixé à CHF 2'000.-- en vertu des art. 5 et 8 al. 1 du règlement du Tribunal pénal fédéral sur les frais, émoluments, dépens et indemnités de la procédure pénale fédérale du 31 août 2010 (RS 173.713.162).

Par ces motifs, la Cour des plaintes prononce:

1. Le recours est rejeté dans la mesure de sa recevabilité.

2. Un émolument de CHF 2'000.-- est mis à la charge du recourant.

Bellinzone, le 26 janvier 2021

Au nom de la Cour des plaintes
du Tribunal pénal fédéral

Le président: La greffière:

Distribution

- Me Maurice Harari et Me Laurent Baeriswyl
- Ministère public de la Confédération

Indication des voies de recours

Il n'existe pas de voies de recours ordinaire contre la présente décision.